**Politica de Segurança da Informação**

Politica de Segurança da Informação

**March de 2023**

Uma **política de segurança da informação** (**PSI**) ou **política de segurança das informações e comunicações** (**PoSIC**) tem por objetivo possibilitar o gerenciamento da segurança de informação em uma organização, estabelecendo regras e padrões para proteção da informação. A política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário. É um elemento essencial para o sucesso de um SGSI (Sistema de Gestão de Segurança da Informação).

A segurança da informação procura proteger diferentes tipos de ameaças para garantir a continuidade dos negócios, reduzir riscos e busca a maximização dos retornos em investimentos e ampliação das oportunidades de negócios.

O conteúdo da política de segurança da informação varia. Entre as organizações, dependendo de seu grau de informatização, de mercado, requisitos de segurança, etc. No entanto, uma política de segurança da informação geralmente inclui a definição de segurança da Informação, seus objetivos e o que compõe. Confia no compromisso da alta administração, define os procedimentos de controle de segurança da informação a serem implementados, como o uso de senhas, as responsabilidades dessa política e as penalidades de sua violação.

Política de segurança da informação é a padronização das normas obrigatórias a fim de manter o controle do comportamentos dos envolvidos para garantir a proteção e as informações da organização. Se tornando semelhante ao Direito, as leis possuem em si definição semelhante as políticas de segurança da informação, e para a avaliação de eficiência e eficácia de uma PSI, quanto a manutenção comportamental, é indicado uma adaptação das teorias de análise comportamental do Direito.

Seu processo de implantação deve resultar na documentação dos procedimentos e sua padronização, também suas ferramentas e técnicas utilizadas. Criando assim indicadores, registros e definindo um processo de conscientização.

Os controles devem ser definidos levando em conta as características de cada empresa, definindo o que é permitido e o que é proibido. A implantação, para ser bem sucedida, deve partir da diretoria da empresa para os demais funcionários (abordagem *top down*). A política deve ser divulgada para todos os funcionários da organização, de forma a manter a segurança das informações.

Um método importante de avaliar em segurança da informação o quanto o comportamento de seu profissional é seguro ou perigoso aos dados e ativos de uma empresa leva em conta[[1]](fontTable.xml);

a susceptibilidade a ameaças por parte do funcionário;

a severidade das ameaças que ele possa vir a receber;

a certeza da detecção por parte da POSIC;

a severidade da punição;

o esforço de salvaguarda;

a satisfação do funcionário.

## Norma ISO/IEC TR 13335

A norma ISO/IEC é um exemplo de uma norma de técnicas muito utilizada para gestão de segurança na área de tecnologia da informação. Ela é utilizada junto de outras normas como a [BS 7799-2](theme/theme1.xml), sendo essa uma norma que sugere quais os processos devam ser implementados. Dentre suas técnicas estão a criação de um comitê multidisciplinar que se reúna para avaliar os níveis aceitáveis de risco e cobrança e uma lista extensa de contramedidas em diferentes situações.